

SEALED

U.S. DISTRICT COURT  
NORTHERN DISTRICT OF TEXAS  
FILED  
OCT 23 2019  
CLERK, U.S. DISTRICT COURT  
By Sud  
Deputy

UNITED STATES DISTRICT COURT

for the  
Northern District of Texas

In the Matter of the Search of

Information Associated with Login Account ID  
DCanchola@yahoo.com  
as described in Attachment A, that are stored at premises  
controlled by DocuSign, Inc.

Case No. 3:19-MJ-948-BN

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment A

located in the Northern District of Texas, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. Secs. 371, 1347, 1349 and 42 U.S.C. Sec. 1320a-7b	Conspiracy to Defraud the United States and to Pay and Receive Health Care Kickbacks; Health Care Fraud; Conspiracy to Commit Health Care Fraud; and Anti-Kickback Statute.

The application is based on these facts:  
See Attachment Affidavit of HHS Special Agent Matthew Kirk

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Matthew Kirk  
Applicant's signature

Matthew Kirk, Special Agent  
Printed name and title

Sworn to before me and signed in my presence.

Date:

10/23/19

David L. Horan  
Judge's signature

David L. Horan, United States Magistrate Judge  
Printed name and title

City and state: Dallas, Texas

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT**

I, Matthew Kirk, a Special Agent with the United States Department of Health and Human Services, Office of Inspector General (“HHS-OIG”), being duly sworn, depose and state under oath the following:

**A. INTRODUCTION**

1. I make this affidavit in support of an application pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703, for a warrant to search all records, data, and information associated with a certain Target Account associated with Dr. Daniel Ramiro Canchola, login Account ID “Dcanchola@yahoo.com” (the “Target Account”) that are electronically stored at premises owned, maintained, controlled, or operated by DocuSign, Inc. (“DocuSign”), an electronic platform that facilitates sharing and e-signature of electronic documents and remote storage of documents with a registered agent located at Corporation Service Company, 300 Deschutes Way SW, Suite 304, Tumwater, WA 98501 (“Subject Premises”), more fully described in Attachment A, and to seize items described in Attachment B.

2. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require DocuSign to disclose to the Government copies of records and information in its possession pertaining to the subscriber or customer associated with the accounts, including the content of communications as further described in Section I of Attachment

B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

**B. IDENTITY AND EXPERIENCE OF AFFIANT**

3. I am a Special Agent of the United States Department of Health and Human Services-Office of Inspector General (“HHS-OIG”) and have been employed as a Special Agent since October 2010. As such, my duty is to conduct criminal and civil investigations involving programs and operations of the Department of Health and Human Services, including both Medicare and Medicaid fraud. Before joining HHS-OIG, I worked as a SA for the United States Department of State, Diplomatic Security Service (“DSS”) from October 2001 until October 2010. My duties at DSS included conducting criminal investigations involving passports, visas, identity theft, illegal immigration and the investigation of Department of State employees. During my approximately 18 years as a Special Agent, I have participated in hundreds of criminal investigations. I regularly participate in the execution of search warrants for documents and other evidence in cases involving violations of federal law, including 18 U.S.C. § 371 (Conspiracy), 18 U.S.C. § 1035 (False Statements Relating to Health Care Matters), 18 U.S.C. § 1347 (Health Care Fraud), 18 U.S.C. § 1349 (Conspiracy to Commit Health Care Fraud and/or Wire Fraud), 18 U.S.C. § 1343 (Wire Fraud), and 42 U.S.C. § 1320a-7b (Anti-Kickback Statute). I have been a member of the Dallas Medicare Fraud Strike Force since 2010.



**C. PURPOSE OF THE AFFIDAVIT**

4. As described more fully below, there is probable cause to believe that located in the Target Account there exists evidence of crimes, fruits of crimes, contraband, and other items illegally possessed in violation of federal laws, including 18 U.S.C. § 371 (Conspiracy to Defraud the United States and to Pay and Receive Health Care Kickbacks), 18 U.S.C. § 1035 (False Statements Relating to Health Care Matters), 18 U.S.C. § 1347 (Health Care Fraud), 18 U.S.C. § 1349 (Conspiracy to Commit (Conspiracy to Commit Health Care Fraud and/or Wire Fraud), 18 U.S.C. § 1343 (Wire Fraud), and 42 U.S.C. § 1320a-7b (Anti-Kickback Statute), as more fully described in Attachment B.

5. The statements in this affidavit are based upon information I learned during the investigation, information provided to me by investigative personnel of the HHS-OIG, as well as from public sources and business records and my experience and background as a Special Agent.

6. Because this affidavit is being submitted for the limited purpose of obtaining a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of crimes, fruits of crimes, contraband, and other items illegally possessed, in violation of federal laws, including 18 U.S.C. §§ 371, 1035, 1347, and 1349, and 42 U.S.C. § 1320a-7b, are currently located in the Target Account.



**D. THE MEDICARE PROGRAM**

7. Medicare is a federally funded health insurance program that provides health benefits to individuals who are 65 years of age or older or disabled, and it is a “health care benefit program,” as defined by Title 18, United States Code, Section 24(b). Medicare is administered by HHS through its agency, the Centers for Medicare and Medicaid Services (“CMS”).

8. Individuals who receive benefits under Medicare are referred to as Medicare “beneficiaries.” Beneficiaries are eligible to receive a variety of services, including hospital services (“Part A”), physician services (“Part B”), and prescription drug coverage (“Part D”). Part B covers outpatient physician services, such as office visits, minor surgical procedures, and laboratory services, such as drug testing and genetic testing, when certain criteria are met.

9. “Providers” include clinical laboratories, physicians, and other health care providers who provide services to beneficiaries. In order to bill Medicare, a provider must submit an enrollment application to Medicare. The enrollment application contains certification statements that the provider must agree to before enrolling with Medicare. Specifically, the certification statement sets forth, in part, that the provider agrees to abide by the Medicare laws, regulations, and program instructions and will not knowingly present or cause to be presented a false or fraudulent claim for payment by Medicare.

10. A Medicare “provider number” is assigned to a provider upon approval of the provider’s Medicare application. A provider may use that provider number to file

claims with, or “bill” Medicare to obtain reimbursement for services rendered to beneficiaries.

11. Medicare contracts with private companies in various jurisdictions to process claims, determine coverage rules, and provide reimbursement.

12. This investigation concerns claims submitted to Medicare for Part B laboratory services, namely, cancer genetic testing.

13. The Social Security Act, Title 42, United States Code, Section 1395y(a)(1)(A) states that no Medicare payment shall be made for items or services that “are not reasonable and necessary for the diagnosis or treatment of illness or injury or to improve the functioning of malformed body member.” As a condition of Medicare payment, a physician or other Medicare provider must certify that the services performed were medically necessary. 42 U.S.C. § 1395n(a)(2)(B).

14. Further, Title 42, Code of Federal Regulations, Section 410.32(a) provides, “All diagnostic x-ray tests, diagnostic laboratory tests, and other diagnostic tests must be ordered by the physician who is treating the beneficiary, that is, the physician who furnishes a consultation or treats a beneficiary for a specific medical problem and who uses the results in the management of the beneficiary's specific medical problem.” “Tests not ordered by the physician who is treating the beneficiary are not reasonable and necessary.” *Id.*

15. When submitting claims to Medicare for reimbursement, providers certify that: (1) the contents of the forms are true, correct, and complete; (2) the forms are

prepared in compliance with the laws and regulations governing Medicare; and (3) the services purportedly provided, as set forth in the claims, are medically necessary.

**E. TARGET OFFENSES**

**Health Care Fraud**

16. Title 18, United States Code, Section 1347 prohibits health care fraud. It provides, “Whoever knowingly and willfully executes, or attempts to execute, a scheme or artifice—

- a. to defraud any health care benefit program; or
- b. to obtain, by means of false or fraudulent pretenses, representations, or promises, any of the money or property owned by, or under the custody or control of, any health care benefit program,

in connection with the delivery of or payment for health care benefits, items, or services, shall be fined under this title or imprisoned not more than 10 years, or both.”

17. Title 18, United States Code, Section 1349 provides that any person who attempts or conspires to commit health care fraud shall be subject to the same penalties as those set forth in Title 18, United States Code, Section 1347.

18. Title 18, United States Code, Section 24(b) defines a “health care benefit program” as “any public or private plan . . . affecting commerce, under which any medical benefit, item, or service is provided to any individual, and includes any individual or entity who is providing a medical benefit, item, or service, for which payment may be made under the plan.”



**Federal Anti-Kickback Statute**

19. The Federal Anti-Kickback Statute, Title 42, United States Code, Section 1320a-7b, prohibits the payment or receipt of “any remuneration” in exchange for “referring an individual to a person for the furnishing or arranging for the furnishing of any item or service for which payment may be made in whole or in part under a Federal health care program.”

20. When enrolling as a Medicare provider, physicians, clinical laboratories, and others must certify that they will comply with the Medicare laws, regulations, and program instructions, including the Federal Anti-Kickback Statute.

**F. MEDICARE COVERAGE FOR CANCER GENETIC TESTING**

21. Clinical laboratories offer cancer genetic tests, also referred to as “CGx tests,” in order to identify hereditary cancer risks. These tests can indicate an increased risk of developing certain cancers in the future, but do not detect existing cancer.

22. Medicare regulations provide coverage for certain cancer screening tests of beneficiaries, such as mammograms and colonoscopies. However, cancer genetic testing, which does not screen for existing cancer but indicates a risk of developing certain cancers in the future, is covered by Medicare only when there is a personal history of cancer (as opposed to a family history of cancer), the testing is ordered by a treating physician, and the testing is medically necessary.

23. Medicare publishes guidance regarding what services it does and does not cover in a variety of publications, including National Coverage Determinations (“NCDs”) which are publicly available online.

24. Specifically regarding cancer genetic testing, Medicare issued NCD 90.2 (effective Mar. 16, 2018). Under NCD 90.2, Medicare covers genetic testing as “reasonable and necessary” so long as: the testing is “ordered by a treating physician”; the beneficiary has “either recurrent, relapsed, refractory, metastatic, or advanced stage III or IV cancer”; and the beneficiary has “decided to seek further cancer treatment,” among other requirements. In NCD 90.2, Medicare made it clear to providers that Medicare does not reimburse for genetic testing performed to determine the likelihood that a beneficiary will develop cancer in the future. Rather, Medicare will only pay for genetic testing performed to aid in the treatment of a beneficiary with a current personal diagnosis of cancer.

25. In 2019, the government spoke with a Medicare expert who confirmed that Medicare does not pay for all preventative medicine or screenings. Congress has authorized payment for certain screening tests, such as annual mammograms, colonoscopies, digital prostate exams and annual “wellness” visits, among others. Congress has *not*, however, authorized payment for cancer genetic screening, i.e., testing designed solely to let beneficiaries who have no symptoms of cancer know whether they have mutations that might cause cancer in the future.

26. The Medicare expert further stated that Medicare does not consider cancer genetic testing to be medically necessary unless (i) a beneficiary is currently being treated for cancer or is exhibiting symptoms that the beneficiary's physician believes could be related to a the beneficiary having cancer, (ii) the test is ordered by the physician who is treating the beneficiary for cancer or cancer symptoms, and (iii) the physician who orders the test uses the test results to treat the beneficiary's cancer or cancer symptoms. Medicare does not reimburse for cancer genetic testing in beneficiaries who exhibit no symptoms of cancer.

**G. TELEHEALTH AND MEDICARE**

27. In general, Medicare reimburses providers for a limited number of services furnished by a physician to an eligible beneficiary via telecommunications system. Medicare refers to covered audio/video communication between a physician and a patient as "telehealth." Under certain circumstances, Medicare considers a telehealth physician-patient encounter to be a substitute for an in-person encounter.

28. The pertinent requirements for a provider engaging in Medicare telehealth encounters are as follows:

a. The beneficiary must be at an approved "originating site," using an approved telecommunications system. 42 U.S.C. § 1395m(m)(4)(B).

b. The originating site must be in a county outside of a Metropolitan Statistical Area ("MSA"), or inside a rural Health Professional Shortage Area ("HPSA"). 42 U.S.C. § 1395m(m)(4)(C)(i).



c. The originating sites authorized by law include the offices of physicians or practitioners; hospitals, rural health clinics and their affiliated dialysis centers; federally qualified health centers; and skilled nursing facilities. *Id.*

#### **H. INVESTIGATION BACKGROUND**

29. Since 2015, I have been actively conducting several criminal investigations of various entities engaged in a common genetic testing health care fraud scheme. I know from my training and experience that certain Medicare providers, marketers, and recruiters engage in fraud by convincing Medicare beneficiaries to provide their personal identifying information and genetic sample, which in turn is used to bill Medicare for expensive, medically unnecessary genetic tests. I also know from my training and experience that such Medicare providers, marketers, and recruiters often rely on call centers to market genetic testing kits aggressively to Medicare beneficiaries, regardless of medical necessity. Based on my training and experience, I know that in some cases, the physician who signs the order for the genetic testing does not have any contact with the beneficiary, whether in-person or via telehealth using audio/video communication. Instead, I know from my training and experience that in some cases, these physicians authorize tests—without ever seeing, speaking with, or otherwise examining the beneficiary—in exchange for an illegal kickback.

30. Multiple entities, operating nationwide, are involved in schemes to defraud Medicare through the vehicle of CGx testing. The schemes typically involve the following parts:

a. Marketers identified Medicare beneficiaries and convinced them to provide their Medicare ID number and other personal identifying information (“PII”). To accomplish this, the marketers misrepresented to beneficiaries that, among other things: (i) Medicare wanted the tests administered for all beneficiaries, (ii) there was cost-savings by inflating the medical value of CGx testing, and (iii) thousands die every year from prescription drug interactions gone awry. The marketer then collected a genetic sample, typically the beneficiary’s saliva, via a cheek swab. The beneficiary then signed a virtual form on the marketer’s tablet, acknowledging the release of their PII. After the genetic sample and PII was collected, the marketer typically informed the beneficiary that an unidentified doctor would contact them for a consultation. Occasionally, the marketer also informed the beneficiary that the doctor would contact them to explain any test results. Through my investigation, I have discovered that the beneficiaries who submitted genetic samples and PII were very rarely, if ever, contacted by a physician.

b. After the marketer collected a beneficiary’s genetic sample and PII, a doctor authorized an order for CGx testing. Typically, this physician was purportedly employed by a telehealth company to provide telehealth services. In reality, the doctor rarely consulted with or otherwise treated any of the beneficiaries for whom genetic testing was authorized. A

common part of the scheme was that the doctor signed an electronic order that was generated based on the PII collected by the marketer, in the absence of any physician-patient relationship or contact. The doctor typically signed the electronic form as soon as it was generated, oftentimes simultaneous to the marketer collecting the beneficiary's genetic sample.

- c. The telemedicine physicians were paid per order they sign, usually by the telehealth company or the laboratory that receives the genetic sample and doctor's order.
- d. The beneficiary's genetic sample was then sent to a laboratory. The laboratory conducted the CGx tests and submitted claims to Medicare for reimbursement.
- e. The laboratory used the money from Medicare to compensate the marketing and telehealth companies for the completed swab and doctor's order, and the cycle described above started anew.

31. Of the beneficiaries interviewed who submitted a genetic sample and their PII, I have yet to interview a beneficiary who has actually spoken to any medical professional, nor the physician who signed the order for CGx testing. Instead, all the interviewed beneficiaries recall speaking only with marketers prior to their genetic sample being collected. The vast majority of beneficiaries I have interviewed have not received any results for genetic tests.



**I. PROBABLE CAUSE THAT EVIDENCE OF CRIMES IS STORED/LOCATED IN THE TARGET ACCOUNT**

32. On or about April 29, 2019, I opened an investigation on Dr. Daniel R. CANCHOLA, MD ("CANCHOLA"). A cursory review of Medicare claims data revealed that, when compared with his peers in Texas, CANCHOLA ranked first for referring Medicare beneficiaries for laboratory genetic tests, including CGx tests. From in or about February 1, 2018 to the present, CANCHOLA referred approximately 4,662 Medicare beneficiaries nationwide for CGx testing. Approximately seventeen laboratories submitted claims to Medicare where CANCHOLA was the referring physician. The total amount laboratories billed to Medicare for claims where CANCHOLA was listed as the referring physician is more than approximately \$102 million. Medicare paid laboratories more than approximately \$25 million for these claims.

33. According to Medicare enrollment documents CANCHOLA is a Medicare provider with the National Provider Identifier 1184771347 and a provider mailing address and practice location of 7200 State Highway 161, Suite 300, Irving, Texas 75039.

**Interview and Consent-to-Search Materials**

34. On or about August 20, 2019, I interviewed CANCHOLA. He reported that he has been involved with telemedicine companies since 2010. According to CANCHOLA, he is licensed to practice medicine and credentialed in multiple states because telemedicine patients are within and outside of the state of Texas.

35. CANCHOLA stated that in or about May 2018, he contracted with Michael Nolan and Richard L. Epstein, the owners and operators of telemedicine companies, to sign prescriptions for CGx testing and, among other things, durable medical equipment services.

36. According to CANCHOLA and as confirmed by Secretary of State records, Nolan and Epstein's telemedicine companies are Comprehensive Telcare, LLC ("CT"), and REMN Management, LLC ("REMN"), both located at 13902 N. Dale Mabry Highway, Suite 121, Tampa, Florida 33618.

37. CANCHOLA stated he received emails to his Yahoo email account from CT containing documents that he would access using the software platform DocuSign. These documents included prescriptions, which CANCHOLA referred to as "requisitions," for CGx testing and/or durable medical equipment for beneficiaries across the United States. When CANCHOLA reviewed the requisitions within DocuSign, they were pre-filled and only needed his signature to be completed. He estimated he would spend two to three minutes on each prescription, during which time he would read each form and then click to electronically affix his signature.

38. The signed requisitions were stored within CANCHOLA's DocuSign account. Using his cell phone, CANCHOLA showed me his Yahoo email account, which displayed individual emails with website URL links that he clicked to open several signed prescriptions that he had reviewed and signed in his DocuSign account.

39. CANCHOLA stated he never spoke to, met in person, or swabbed any of the patients associated with CT and/or REMN whose requisition forms he signed. He stated he was not the treating physician or primary care physician for any of those patients, nor did he have any sort of physician-patient relationship with them.

40. CANCHOLA told agents that CT and REMN paid CANCHOLA \$20 to \$30 for each order that he signed. He received these payments by either physical or electronic check.

41. CANCHOLA stated that he stopped signing prescriptions for CT and REMN after he read an article online that said REMN had been sold.

42. On or about August 22 and 23, 2019, CANCHOLA executed an agreement consenting to the search of his Yahoo email account and provided his DocuSign “envelope” login account ID credentials, including Dcanchola@yahoo.com.

#### **Bank Records**

43. A review of bank account records belonging to CANCHOLA reveal that he was paid *at least* approximately \$500,000 by REMN and CT between in or about June 2018 and in or about March 2019.

#### **Hotline Complaints and Beneficiary Interviews**

44. HHS-OIG manages a hotline which accepts complaints from the public via phone or electronic submission (the “hotline”). On or about February 18, 2019, the



hotline received a complaint from the son-in-law of O.W., a Medicare beneficiary who resides in Brandon, Mississippi.

- a. The complainant reported that O.W. had received a Medicare summary notice with claims for various pathology and gene analysis that O.W. had never received. The claim showed CANCHOLA as the referring physician and that Medicare had paid approximately \$10,000 for the claim.
- b. Medicare claims data shows that claims were submitted for O.W. by Suretox Laboratory LLC, with a service date of on or about October 6, 2018. The total amount billed to Medicare was approximately \$10,131.54, and Medicare paid the laboratory approximately \$7,764.14 for the claims.

45. On or about March 5, 2019, the hotline received a complaint from the husband of M.B., a Medicare beneficiary who resides in Austin, Texas. M.B. received a Medicare summary notice showing a laboratory submitted more than twenty claims related to genetics for more than \$17,000 that were referred by CANCHOLA. Of those claims, eight claims were approved by Medicare, and Medicare paid the laboratory approximately \$4,224.12.

- a. Medicare claims data shows that Acadian Diagnostics Laboratories, LLC submitted claims for M.B. with a service date of on or about October 12, 2018. The total amount billed was approximately \$16,780.00, and Medicare paid the laboratory \$0.00 for the claims.

- b. On or about September 10, 2019, agents telephonically interviewed beneficiary M.B., whose husband had previously complained to the HHS hotline on her behalf. M.B. told agents that she received a swab kit in the mail and submitted a saliva sample herself for cancer screening. She was uncertain whether she received the results. M.B. never saw or spoke to CANCHOLA and had never heard of him until seeing his name on the Medicare summary notice.
- c. In the consent-to-search materials, there is a requisition signed by CANCHOLA for M.B. M.B. signed the requisition on August 12, 2018.
- d. Medicare claims data shows that Acadian Diagnostic Laboratories LLC (“Acadian”) billed approximately \$16,780 for claims associated with M.B. and was paid \$0.00.

46. On or about May 1, 2019, the hotline received a complaint from R.W., a Medicare beneficiary who resides in Kaufman, Texas. R.W. reported she received a fraudulent charge on her Medicare account from a physician named Dr. Daniel CANCHOLA for a laboratory called Specialty Drug Testing LLC (“Specialty”). The total amount billed was approximately \$12,786.97, and Medicare paid the laboratory approximately \$6,075.66. R.W. reported that she is not a patient of CANCHOLA, and she did not receive any such testing.

- a. Medicare claims data shows that Specialty submitted claims for a beneficiary believed to be R.W. with a service date of on or about October

20, 2018.<sup>1</sup> The total amount billed was approximately \$14,317.45, and Medicare paid the laboratory approximately \$6,075.66 for the claims.

- b. Agents telephonically interviewed R.W. on or about September 11, 2019. R.W. confirmed she had never heard of or been treated by CANCHOLA.

47. On or about July 31, 2019, I interviewed M.M., who resides in Arlington, Texas. On or about November 15, 2018, M.M. attended a health fair with her husband at the YMCA in Arlington, Texas. She spoke with a representative of a marketing company that advertised genetic testing. The marketer said the tests would be able to tell if someone had a higher risk for cancer or if their children would be at risk. He also told them that another genetic test could determine how a person's body would react to certain medicines. The marketer told M.M. that the tests would be completely paid for by Medicare. M.M. submitted a saliva swab the same day, entered her personal information on a tablet device, and signed a form. The marketer told M.M. that she would receive the test results in six to eight weeks.

- a. In or about April 2019, when M.M. had not received the results, M.M. emailed the medical marketing company's customer service department detailing her disappointment with the process. She also attempted to call the customer service department several times.

---

<sup>1</sup> The name associated with the claims is not an exact match; however, other personal and identifying information on the claims, including the beneficiary's Medicare ID number, matches with the information R.W. reported to the hotline.



- b. M.M. received a Medicare Explanation of Benefits form showing that genetic tests had been billed for approximately \$8,373. CANCHOLA was listed as the referring physician. M.M. does not know CANCHOLA and has not had any in person, telephonic, or electronic communication with him. M.M. has not received any genetic testing results.<sup>2</sup>
- c. Medicare claims data shows that Specialty submitted CGx claims for M.M. with a service date of November 15, 2018. The total billed was approximately \$8,373.18, and Medicare paid the laboratory approximately \$3,838.44 for the claims.

48. On or about August 8, 2019, agents interviewed beneficiaries K.J. and J.J., a married couple residing in Austin, Texas. While vacationing in October 2018 in Ft. Lauderdale, they attended an art fair where there was a vendor with a pop-up tent labeled “Genex Health,” advertising cancer screening and other health tests. J.J. had been diagnosed with cancer in 2012, which was treated by a doctor in Texas. K.J. and J.J. submitted buccal swabs to the associates from Genex. Genex staff asked first if K.J. and J.J. had Medicare and stated their services were free but they had to submit their driver’s licenses and Medicare cards for coverage. The personal information was entered

---

<sup>2</sup> I also interviewed M.M.’s husband, T.M., on the same day, July 31, 2019. T.M. attended the same health fair and submitted a genetic swab sample to a marketer and he did receive genetic test results. However, the prescribing physician was Luis Mojicar, MD, and the explanatory form provided to T.M. indicated that the results were “inconclusive.”

into either an iPad or iPhone. In or about January 2019, J.J. received her Medicare Summary Notice by mail, which revealed that billing had been submitted by Specialty. K.J. and J.J. still had not received any results for either of their testing and then inquired online to review K.J.'s Medicare Summary Notice. They discovered that Specialty had also billed Medicare for K.J.'s test. K.J. and J.J. have never received their test results and did not recognize the name of Dr. Daniel CANCHOLA, the physician who signed off on their tests. Medicare data confirms that Specialty billed CGx testing for K.J. and J.J.

49. On or about September 11, 2019, I interviewed beneficiary I.V. According to I.V., she submitted a genetic sample for cancer testing in about December 2018. After answering a phone call regarding genetic testing, I.V. received a testing kit in the mail. The kit included a swab to collect her saliva sample and a shipping label once the swab and paperwork were completed. I.V. recalled receiving results in about January 2019 but her primary care physician told her the results stated "nothing was indicated." I.V. had never been a patient of Dr. CANCHOLA and had never spoken to him.

- a. A requisition form for CGx testing for I.V., which contained her PII and was signed by CANCHOLA, was identified in the materials voluntarily provided by CANCHOLA.
- b. Medicare claims data confirms that Acadian billed approximately \$11,264 for claims associated with I.V. and was paid approximately \$4,026.91.

50. On or about September 12, 2019, I interviewed beneficiary B.H. B.H. recalled receiving a phone call in 2018 regarding genetic testing and received a testing kit

and forms in the mail after the call. B.H. confirmed his signature on the requisition form and stated that the form already included his personal information when he received it. B.H. explained that he mailed the signed form and a saliva sample he collected himself, using a shipping label provided with the kit. B.H. never received any test results. Despite attempts to call the customer service number he was provided, B.H. indicated that no one ever answered. B.H. also told me that after the genetic testing phone call, he received medical braces through the mail that he never ordered. B.H. stated he never met or had been treated by Dr. CANCHOLA.

- a. A requisition form for CGx testing for B.H., which contained his PII and was signed by CANCHOLA, was identified in the materials voluntarily provided by CANCHOLA.
- b. Medicare claims data confirms that Acadian billed approximately \$23,968 for claims associated with B.H. and was paid approximately \$4,026.91.

**J. PROBABLE CAUSE TO SEARCH THE TARGET ACCOUNT**

51. While agents were given access to the documents maintained by DocuSign through the Yahoo! email consent-to-search executed by CANCHOLA, this warrant seeks authority to seize all data, records, content, and correspondence related to the Target Account so as to preserve the original copy of the evidence, and to identify any information and records related to the Target Account.

52. On or about August 23, 2019, the government served DocuSign, the provider of the Target Account, with a preservation letter under 18 U.S.C. § 2703(f),



requesting that DocuSign preserve all electronically stored information in its possession regarding the Target Account for a period of ninety days. DocuSign has acknowledged receipt of the preservation notice and has agreed to comply.

53. Epstein and others routinely communicated with CANCHOLA via email regarding genetic testing and kickbacks for Medicare beneficiary referrals. These communications included calculating payments CANCHOLA was owed based upon the number of genetic test orders he signed. And, specifically using the Target Account, CANCHOLA received genetic testing requisition forms from Epstein and others, which he electronically signed and sent back a completed version.

54. These communications establish probable cause to believe that the Target Account will contain records and communications relating to the TARGET OFFENSES.

55. As described above, the DocuSign Target Account contains Medicare beneficiary patient records (“records”). The Target Account is hosted on computer services owned, maintained, controlled, and/or operated by DocuSign. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require DocuSign to disclose to the government, records and other information in its possession pertaining to the documentation stored in DocuSign and communications between DocuSign and CANCHOLA, and CANCHOLA and CT, REMN, Epstein, and others. Attachment A describes the records, and Attachment B further describes the information the government seeks to seize.

**K. TECHNICAL BACKGROUND AND ITEMS LIKELY TO BE FOUND**

56. DocuSign is a cloud business service that hosts a multitude of digital signature services and various cloud services, including the document storage used by the Target Account to sign, store and transfer documents between CANCHOLA and CT.

57. In general, providers like DocuSign ask each of their subscribers to provide certain information when registering for an account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, email addresses, and, for paying subscribers, a means and source of payment (including any creditor bank account number). Providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access.

58. In some cases, account users will communicate directly with a provider about issues relating to their account, such as technical problems, billing inquiries, or

complaints from other users. Providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

59. This application seeks a warrant to search all responsive patient records, communication records and information under the control of DocuSign, a provider subject to the jurisdiction of this court, regardless of where DocuSign has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within DocuSign's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

**L. SEALING AND NON-DISCLOSURE ORDER**

60. This investigation is ongoing. Premature disclosure of the Applications and Affidavit for Search Warrants may compromise the investigation by, among other things, disclosing the precise matters being reviewed and the status of the investigation to date. Accordingly, it is respectfully requested that the Applications and Affidavit for Search Warrants be sealed until further Order of the Court.

61. Pursuant to Title 18, United States Code, Section 2705(b), it is also respectfully requested that the Provider be ordered not to notify any other person



regarding the existence of the search warrants (“Non-Disclosure”). Non-Disclosure is justified because the search warrants relate to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and disclosure may alert the target(s) and others to the ongoing investigation. Accordingly, there is reason to believe that disclosure of the search warrants will seriously jeopardize the investigation, including by giving the target(s) and others an opportunity to flee, destroy or tamper with evidence, intimidate potential witnesses, or otherwise seriously jeopardizing the investigation. *See* 18 U.S.C. § 2705(b). It is therefore respectfully request that the Court order Non-Disclosure, with the following exceptions:

- a. for the purpose of receiving legal advice, the Provider may disclose the Non-Disclosure Order to an attorney for the Provider;
- b. for the purpose of making statistical reports (also known as “transparency reports”), the Provider may disclose the fact that an order under 18 U.S.C. § 2703(d) was received, the date of issuance, and court of issuance, provided that the Provider does not disclose the targeted account(s); and
- c. the Provider may disclose this search warrant one year after the date of the Non-Disclosure Order, but only if (1) the Provider has not received an order extending the period of non-disclosure for this warrant, and (2) the Provider has provided the Government with 15 days’ notice before disclosing this warrant. *See* 18 U.S.C. § 2705(b).

**M. RETENTION OF INFORMATION FOR AUTHENTICATION**

62. In anticipation of litigation relating to the authenticity of data seized pursuant to the Warrants, the Government requests that it be allowed to retain a digital copy of all seized information authorized by the Warrants for as long as is necessary for authentication purposes.

**N. CONCLUSION**

63. Based upon all the facts set forth above, there is probable cause that evidence, fruits and property used to commit the crime of False Statements Relating to Health Care Matters in violation of Title 18, United States Code, Section 1035, Health Care Fraud, in violation of Title 18, United States Code, Section 1347, Conspiracy to Commit Health Care Fraud, in violation of Title 18, United States Code, Section 1349, Conspiracy to Commit an Offense against the United States, in violation of Title 18, United States Code, Section 371, and Paying and/or Receiving Health Care Kickbacks in violation of the Anti-Kickback Statute, Title 42, United States Code, Section 1320a-7b, is present in the Target Account.

64. Further, I submit that there is probable cause to believe that evidence, fruits and instrumentalities of these crimes, as described above and in Attachment B, are located at the location described in Attachment A.

65. In consideration of the foregoing, I respectfully request that this Court issue a search warrant for the Target Account located at the Subject Premises authorizing the search of that location, as described more fully in Attachment A, and the seizure of items

described in Attachment B. Because the warrants will be served on the Providers who will then compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

(Continued on the next page.)

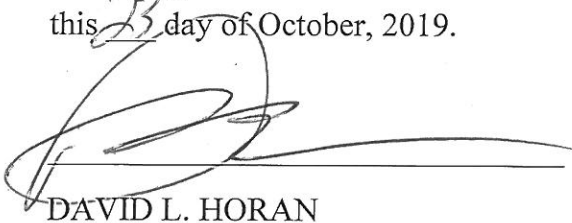


I declare under penalty of perjury that the foregoing is true and correct to the best of my belief and knowledge this 22 day of October, 2019, in Dallas, Texas.



Matthew Kirk  
Special Agent  
U.S. Department of Health and Human Services  
Office of Inspector General

Subscribed and sworn to me before  
this 23<sup>rd</sup> day of October, 2019.

  
DAVID L. HORAN

UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

Property to be searched:

This warrant applies to information and data associated with certain Target Account associated with login account ID credentials "Dcanchola@yahoo.com" that are electronically stored at premises owned, maintained, controlled, or operated by DocuSign, Inc. ("DocuSign"), an electronic platform that facilitates sharing and e-signature of electronic documents and remote storage of documents with a registered agent located at Corporation Service Company, 300 Deschutes Way SW, Suite 304, Tumwater, WA 98501.

**ATTACHMENT B**

Particular Things to be Seized:

**I. INFORMATION TO BE DISCLOSED BY DOCUSIGN, INC. (“DOCUSIGN”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of DocuSign, including any messages, records, files, logs, or information that have been deleted but are still available to DocuSign, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), DocuSign is required to disclose the following information to the Government for each account or identifier listed in Attachment A:

- a. The contents of all documents associated with each account, from January 1, 2016 to the present, including stored or preserved copies of documents and content sent to and from the account, draft documents, the source and destination addresses associated with each document, the date and time at which each document was sent, and the size and length of each document;
- b. all records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses or login information provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number, front and/or back copies of payment instruments, and signatures on payment instruments);

- c. complete account profile information, including names, addresses, and identification numbers, including for DocuSign Envelope IDs and Signature IDs;
- d. all records or other data regarding recipient authentication information;
- e. all records or other data regarding a complete audit trail;
- f. all correspondence and account notes;
- g. all records pertaining to the types of service utilized by the user;
- h. all records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and
- i. all records pertaining to communications between the DocuSign and any person regarding the account, including correspondence, account notes, and contacts with support services and records of actions taken.
- j. the Provider is hereby ordered to disclose the above information to the Government within 14 days of service of this warrant.
- k. for purposes of authentication at trial, the Government is authorized to retain a digital copy of all seized information authorized by the Warrant for as long as is necessary for authentication purposes.

## **II. INFORMATION TO BE SEIZED BY THE GOVERNMENT**

All information described above in Section I that constitutes evidence, fruits, or instrumentalities of violations of 18 U.S.C. §§ 1035, 1343, 1347, 1349, 371, and 42 U.S.C. § 1320a-7b, those violations involving Dr. Daniel R. CANCHOLA occurring after



January 1, 2016, to the present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

1. All communications, records, and documents related to prescriptions for durable medical equipment and genetic testing (referred to in the attached Affidavit as “requisitions”) and medical records marketing services, genetic testing, and medical information of past, present, or future physical or mental health conditions; the past, present, or future provision of health care; or the past, present, or future payment for the provision of health care services, involving Dr. Daniel CANCHOLA, Richard Epstein, Michael Nolan, Comprehensive Telcare, LLC (“CT”), and REMN Management, LLC (“REMN”) and their employees and contractors.

2. Evidence indicating how and when DocuSign was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner.

3. Evidence indicating the account owner’s state of mind as it relates to the crime under investigation.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review any information provided pursuant to this search warrant in order to locate the things particularly described in this warrant.

### **III. SPECIAL INSTRUCTION REGARDING REVIEW OF THE SEIZED MATERIAL**

With respect to law enforcement's review of the records and information described in Section II (the "Seized Material"), law enforcement (i.e., the federal agents and prosecutors working on this investigation and prosecution), along with other government officials and contractors whom law enforcement deems necessary to assist in the review of the Seized Material (collectively, the "Review Team") are hereby authorized to review, in the first instance, the Seized Material and the information and materials contained in them, as set forth in this Attachment B.

If law enforcement determines that all, some, or a portion of the information or materials within the Seized Material contain or may contain information or material subject to a claim of attorney-client privilege or work-product protection (the "Potentially Privileged Materials"), the Review Team is hereby ordered to: (1) immediately cease its review of the specific Potentially Privileged Materials at issue; (2) segregate the specific Potentially Privileged Materials at issue; and (3) take appropriate steps to safeguard the specific Potentially Privileged Materials at issue.

Nothing in this addendum shall be construed to require law enforcement to cease or suspend the Review Team's review of the Seized Material upon discovery of the existence of Potentially Privileged Materials.